



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'Intérieur

PGSN – A08

Exploitation des systèmes d'information

Version 1.0

Préambule

Le présent document est une composante à part entière de la politique générale de sécurité numérique du ministère de l'Intérieur (PGSN-MI).

Les principes stratégiques de la PGSN-MI et les dispositions générales de l'instruction sont traduits au sein du présent document en objectifs à atteindre, reprenant la structure de la politique de sécurité des systèmes d'information de l'Etat (PSSI-E).

Des règles techniques ou non techniques permettant de contribuer à la réalisation de chaque objectif sont énoncées au sein du présent document :

- Les mesures préfixées par « PSSI- », suivies de la nomenclature seule, sont des règles inchangées de la PSSI de 2014. Des modifications peuvent néanmoins y être effectuées sur l'appellation de certaines fonctions propres au ministère.
- Les mesures préfixées « MI- » sont des mesures venant préciser la règle originale ou définir des règles propres au ministère de l'Intérieur, formulées par le SHFD.

Toute dérogation à un objectif ou une règle du présent document, doit se faire en conformité avec la règle *MI-ORG-PGSN-DEROG* du document [PGSN-A01] du corpus de la sécurité numérique.

Dans la suite du document, le terme « DSI ministérielles » regroupe la direction du numérique et le service des technologies et des systèmes d'information de la sécurité intérieure.

Exploitation des SI

1. Protection des informations sensibles

Objectif A8-1 : protection des informations sensibles. Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.

PSSIE-EXP-PROT-INF : protection des informations sensibles en confidentialité et en intégrité. Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité. A défaut d'utiliser un réseau homologué, ces informations doivent être protégées à l'aide d'un moyen de chiffrement labellisé.

MI-DEV-DON-TST : protection des données de tests. Les données utilisées lors des tests doivent être sélectionnées avec soin, protégées et contrôlées, afin de ne pas conduire au non-respect des réglementations applicables aux données ou à leurs expositions aux risques de compromission. Si la désensibilisation des données de tests n'est pas possible, l'usage des données doit être soumis à la validation du CSN.

MI-EXP-PROT-DCP : protection des données à caractère personnel. Toute entité du ministère de l'Intérieur doit tout mettre en œuvre pour garantir la protection des données à caractère personnel¹ amenées à faire l'objet d'un traitement, conformément à la réglementation européenne applicable². De la même manière, l'ensemble des agents du ministère doivent observer les règles d'hygiène élémentaires quant au traitement des informations personnelles. Ces dernières ne doivent pas être communiquées sur des réseaux non sécurisés et inappropriés, tels des médias sociaux (Facebook, Twitter, LinkedIn, WhatsApp...)³.

2. Sécurité des ressources informatiques

Objectif A8-2 : surveillance et configuration des ressources informatiques. Durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci.

MI-EXP-TRAC : traçabilité des interventions sur le système. Les interventions de maintenance sur les ressources informatiques du ministère doivent être tracées par les services informatiques. Ces données doivent être conservées pour une durée d'un an et être accessibles à la chaîne fonctionnelle SN pour contrôle.

MI-EXP-CONFIG : configuration des ressources informatiques. Les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement, préalablement à leur mise en service. Par ordre de priorité, les référentiels à prendre en considération sont les guides techniques ANSSI, les spécifications techniques ministérielles et les guides de sécurisation des éditeurs. Le CSN doit contrôler la bonne application des procédures de sécurisation.

¹ Informations disponibles sur le site : <http://sg.minint.fr/index.php/rgpd/accueil-les-donnees-personnelles>

² Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016.

³ Liste de réseaux sociaux non exhaustive. Pour plus de détails, se référer au guide de la DICOM relatif au bon usage des réseaux sociaux à destination des agents du ministère : <http://dicom.minint.fr/index.php/web/reseaux-sociaux-et-nouveaux-usages-du-web/guide-du-bon-usage-des-medias-sociaux>

PSSIE-EXP-DOC-CONFIG : documentation des configurations. La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.

3. Gestion des autorisations et contrôle d'accès logique aux ressources

Objectif A8-3 : autorisations et contrôles d'accès. Authentifier les usagers et contrôler leurs accès aux ressources des SI du ministère, en fonction d'une politique explicite d'autorisations.

3.1. Contrôle des accès logiques

MI-EXP-ID-AUTH : identification, authentification et contrôle d'accès logique. L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas de l'accès à des données sensibles, de moyens d'authentification forte doivent être utilisés. A cette fin, l'usage d'une carte à puce doit être privilégié ; à défaut, si l'usage d'un mot de passe est indispensable, sa complexité doit être conforme aux bonnes pratiques.

Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé de gestion des arrivées et des départs, cohérent avec les règles en vigueur au niveau des ressources humaines.

MI-EXP-AUTH : authentification des utilisateurs. L'authentification des utilisateurs est assurée en priorité au travers des portails ministériels authentifiant, homologués et référencés par la MGMSIC. Dans tous les cas, l'authentification forte (notamment au moyen de la carte agent) doit être privilégiée.

PSSIE-EXP-DROITS : droits d'accès aux ressources. Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants :

- Besoin d'en connaître : Chaque utilisateur, exploitant et administrateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès ;
- Moindre privilège : Chaque utilisateur, exploitant ou administrateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui.

PSSIE-EXP-PROFILS : gestion des profils d'accès aux applications. Les applications manipulant des données sensibles doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

MI-EXP-DROITS-RETRAIT : processus de retrait des droits d'accès. Un processus centralisé doit garantir l'adaptation des droits d'accès des utilisateurs qui ont changé de fonction ou de poste et la suppression ou le blocage immédiat des droits d'accès des utilisateurs qui ont quitté l'organisation.

3.2. Processus d'autorisation

MI-EXP-PROC-AUTH : autorisations d'accès des utilisateurs. Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI, qu'elle soit locale ou nationale, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel. Les comptes sont individuels afin de garantir la traçabilité des actions.

MI-EXP-PROC-FONCT : compte fonctionnel d'accès. Lorsqu'un compte fonctionnel est indispensable au fonctionnement d'un service, des mécanismes supplémentaires de traçabilité sont mis en place de sorte que le CSN puisse effectuer des contrôles réguliers sur les actions réalisées. Les mots de passe de ce type de compte doivent être renouvelés tous les 6 mois.

Il est fortement recommandé que le renouvellement du mot de passe soit réalisé à chaque départ d'un utilisateur du compte fonctionnel.

MI-EXP-PRIV-CONTR : création, modification et contrôle d'un compte à privilèges. La création d'un compte à privilèges doit être liée à une demande d'habilitation validée par le propriétaire du service SI concerné. La demande de création d'un compte à privilège doit être validée par le responsable du bénéficiaire.

La modification d'un compte à privilèges est traitée de façon formalisée et fait l'objet de contrôle contradictoire.

MI-EXP-REVUE-AUTH : revue des autorisations d'accès. Une procédure de revue des autorisations d'accès de chaque compte doit être formalisée et réalisée annuellement (il est fortement recommandé que ces revues soient réalisées a minima 2 fois par an) sous le contrôle du CSN, le cas échéant avec l'appui d'un assistant local à la SN ou d'un officier de sécurité.

3.3. Gestion des authentifiants

MI-EXP-CONF-AUTH : confidentialité des informations d'authentification. Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) sont des données sensibles. Ces informations particulières doivent faire l'objet de mesures de protection adaptées.

MI-EXP-GEST-PASS : gestion des mots de passe. Les utilisateurs et administrateurs ne doivent pas stocker leurs mots de passe en clair sur leur poste de travail. Un coffre-fort numérique, labellisé par l'ANSSI, doit être utilisé par l'agent pour faciliter sa gestion des mots de passe. Le stockage des mots de passe sur des supports amovibles est à proscrire sauf pour des besoins de continuité d'activité qui devront mettre en œuvre des mesures adaptées pour garantir la confidentialité des authentifiants ainsi stockés.

MI-EXP-PROC-RES : Protection des mots de passe sur les réseaux. Les mécanismes d'authentification doivent protéger du rejeu en cas d'interception des authentifiants. A ce titre, ces derniers ne doivent pas transiter en clair sur les réseaux ou être protégés par des moyens triviaux. Les mécanismes d'authentification doivent mettre en œuvre des algorithmes cryptographiques conformes aux annexes B du référentiel général de sécurité de l'ANSSI.

MI-EXP-CPT-SERVICE : gestion des authentifiants des comptes de service. Les règles de gestion de mots de passe des comptes de service sont à minima identiques aux comptes utilisateurs. Une attention particulière doit être portée à l'échange du mot de passe et au renouvellement périodique de ces authentifiants. Toute tentative de connexion en échec sur ces comptes doit faire l'objet d'une détection et d'une alerte.

MI-EXP-DEF-PASS : modification des mots de passe par défaut. Les mots de passe par défaut des comptes techniques et applicatifs doivent être modifiés avant la mise en production du système.

PSSIE-EXP-INIT-PASS : initialisation des mots de passe. Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.

MI-EXP-DELIV-MDP : Sécurisation de la délivrance des mots de passe. La délivrance des identifiants et mots de passe (y compris lors du renouvellement de mot de passe) doit suivre une procédure documentée permettant de s'assurer que le couple est délivré à la bonne personne ou à la bonne machine, y compris dans le cas d'un compte temporaire.

PSSIE-EXP-POL-PASS : politiques de mots de passe. Les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures nationales, telles qu'éditées par les maîtrises d'ouvrage nationales, doivent être respectées dans chaque entité. Pour les ressources dont la politique de mots de passe est gérée localement, les recommandations de l'ANSSI doivent être appliquées pour tous les comptes.

MI-EXP-CERTIFS : utilisation de certificats électroniques. L'utilisation de certificats électroniques doit respecter les règles édictées par le RGS (arrêté 10 juin 2015)⁴. Pour des systèmes d'information interne, les IGC ministérielles signées par l'IGC/A doivent être privilégiées. Pour des systèmes d'information mis à disposition du citoyen sur Internet, les certificats électroniques doivent être acquis uniquement auprès de prestataires de service de certificats électroniques qualifiés par l'ANSSI (PSCE).

PSSIE-EXP-QUAL-PASS : contrôle systématique de la qualité des mots de passe. Des moyens techniques permettant d'imposer la politique de mots de passe (par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux) doivent être mis en place. A défaut, un contrôle périodique des paramètres techniques relatifs aux mots de passe doit être réalisé.

3.4. Gestion des authentifiants d'administration

PSSIE-EXP-SEQ-ADMIN : séquestre des authentifiants « administrateur ». Les authentifiants permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. L'authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites. Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit. Les informations d'authentification bénéficiant d'un moyen de protection physique (notamment, carte à puce) n'ont, par défaut, pas besoin d'être l'objet d'opérations de séquestre de la part d'autres personnels que l'authentifié lui-même.

MI-EXP-POL-ADMIN : politique de compte et de mots de passe « administrateurs ». Chaque administrateur doit disposer d'un compte nominatif et d'un mot de passe propre, uniquement destiné à l'administration et distinct de son compte bureautique. Lorsqu'un compte fonctionnel ou de service système est indispensable, des mécanismes complémentaires de traçabilité sont mis en œuvre et le renouvellement du secret est réalisé régulièrement ou à chaque départ d'un utilisateur du compte fonctionnel.

PSSIE-EXP-DEP-ADMIN : gestion du départ d'un administrateur des SI. En cas de départ d'un administrateur disposant de privilèges sur des composants des SI, les comptes individuels dont il disposait doivent être immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (exemples: mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).

⁴ <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030744009/>

MI-EXP-ACC-MFA : authentification multi facteurs des comptes d'admin. Il convient de privilégier l'usage de la carte agent pour tous les accès aux fonctionnalités d'administration.

4. Exploitation sécurisée des ressources informatiques

Objectif A8-4 : sécurisation de l'exploitation. Fournir aux administrateurs les outils nécessaires à l'exercice des tâches de sécurité numérique et configurer ces outils de manière sécurisée.

4.1. Administration des systèmes

MI-EXP-RESTR-DROITS : restriction des droits. Sauf exception dûment motivée et validée par le CSN :

- Les utilisateurs n'ont pas de droits d'administration sur les systèmes ;
- Les personnels d'exploitation et d'administration des systèmes ont des droits à haut privilèges limités au strict nécessaire (Par ex : configuration des sudoers, ...) et l'accès au compte « root » ne doit pas être autorisé sans une procédure de contrôle adaptée.

PSSIE-EXP-PROT-ADMIN : protection des accès aux outils d'administration. L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès. Des annuaires dédiés aux comptes d'administration doivent être mis en œuvre.

PSSIE-EXP-HABILIT-ADMIN : habilitation des administrateurs. L'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation.

MI-EXP-RES-ADMIN : ressources d'administration dédiées. Les ressources matérielles et logicielles des systèmes d'information d'administration sont utilisées exclusivement pour réaliser des opérations d'administration. Les tâches d'administration doivent être réalisées avec un compte dédié et à partir d'un poste spécifique, sans connexion à Internet ou à la messagerie. Si cette disposition ne peut être respectée, un environnement d'administration logiquement isolé pourra être envisagé, avec mise en œuvre de mécanismes de cloisonnement et de conteneurisation.

PSSIE-EXP-GEST-ADMIN : gestion des actions d'administration. Les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

MI-EXP-SEC-FLUXADMIN : sécurisation des flux d'administration. Les opérations d'administration sur les ressources locales d'une entité doivent s'appuyer sur des protocoles sécurisés. Les flux d'administration sont protégés par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'ANSSI.

MI-EXP-INT-ADMIN : Interfaces d'administration et de production distinctes. Les interfaces d'administration et de production sont distinctes ou bien des mesures complémentaires sont mises en œuvre pour protéger l'accès aux ressources d'administration du système.

MI-EXP-RESEAU-ADMIN : sécurisation des réseaux d'administration. Un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs, doit être mis en œuvre. Dans l'optique d'un cloisonnement logique, le déploiement de VPN IPsec doit être privilégié.

MI-EXP-CENTRAL : centraliser la gestion du système d'information. Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.

Pour les systèmes d'information hébergées dans les centres informatiques du ministère de l'Intérieur, les DSI ministérielles mettront en œuvre des infrastructures de gestion centralisée permettant la gestion centralisée des politiques de sécurité, la télédistribution des correctifs de sécurité et des socles logiciels, ainsi que la supervision nationale des configurations. La DNUM et le ST(SI)² mettront respectivement en œuvre des infrastructures similaires pour la gestion centralisée des postes de travail Windows et Linux.

L'ensemble des services du ministère de l'Intérieur doit se raccorder impérativement à ces infrastructures de gestion centralisé.

MI-EXP-SECX-DIST : sécurisation des outils de prise de main à distance. La prise de main à distance d'une ressource informatique locale ne doit être réalisable que par les agents autorisés par l'équipe locale chargée des SI, sur les ressources informatiques de leur périmètre. Des mesures de sécurité spécifiques doivent être définies et respectées. Dans ce domaine, l'application des préconisations des guides ANSSI est obligatoire.

MI-EXP-ADMIN-TMA : accès distant aux ressources d'administration. Les accès distants, hors des locaux du ministère, aux ressources d'administration doivent être réalisés exclusivement à l'aide de solutions homologuées et validées par le HFD.

MI-EXP-ADMIN-TMAEXT : maintenance externalisée. Lorsque l'administration d'un système d'information est confiée à un prestataire externe, les services doivent privilégier les interventions sur site pour lesquelles l'administration doit fournir les postes d'administration. Si cela n'est pas possible, notamment pour les interventions en heures non ouvrées, seules sont autorisées les solutions d'accès distants homologuées et validées par le HFD. En aucun cas, une interconnexion avec le réseau du prestataire ou la connexion de ses outils informatiques ne doit être acceptée.

4.2. Administration des domaines

PSSIE-EXP-DOM-POL : définir une politique de gestion des comptes du domaine. Une politique explicite de gestion des comptes du domaine doit être documentée.

MI-EXP-DOM-PASS : configurer la stratégie des mots de passe des domaines. La politique de gestion des mots de passe doit être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe, ainsi qu'un nombre de tentatives d'authentification avant le verrouillage du compte, doivent être imposés aux utilisateurs. Un renouvellement semestriel doit également être appliqué.

PSSIE-EXP-DOM-NOMENCLAT : définir et appliquer une nomenclature des comptes du domaine. La gestion des comptes doit s'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage : comptes d'utilisateur standard, comptes d'administration (domaine, serveurs, postes de travail) et comptes de service.

PSSIE-EXP-DOM-RESTADMIN : restreindre au maximum l'appartenance aux groupes d'administration du domaine. L'appartenance aux groupes du domaine ADMINISTRATEURS DE L'ENTREPRISE et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

PSSIE-EXP-DOM-SERV : maîtriser l'utilisation des comptes de service. Les comptes de service ont la particularité d'avoir généralement leurs mots de passe inscrits en dur dans des applications ou dans des systèmes. Afin de pouvoir être en mesure de changer ces mots de passe en urgence, il est nécessaire de maîtriser leur utilisation.

PSSIE-EXP-DOM-LIMITSERV : limiter les droits des comptes de service. Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

MI-EXP-DOM-GEST : gestion des domaines Windows Active Directory. L'administration des domaines Windows Active Directory impose une rigueur de gestion et de respect des règles de sécurité par tous les administrateurs, quels que soient leur rôle et leur périmètre de responsabilité. Il est obligatoire de mettre en œuvre les principes de gestion décrits dans les procédures d'exploitation de la sécurité élaborée par la DNUM⁵.

MI-EXP-DOM-OBSOLETE : désactiver les comptes du domaine obsolètes. Il est obligatoire de désactiver immédiatement, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine.

MI-EXP-DOM-ADMINLOC : améliorer la gestion des comptes d'administrateur locaux. Afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes. Pour les solutions Windows, la solution de protection LAPS doit être mise en œuvre.

4.3. Envoi en maintenance et mis au rebut

PSSIE-EXP-MAINT-EXT : maintenance externe. Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Les opérations de chiffrement doivent faire appel à des produits qualifiés. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies en concertation avec l'ANSSI.

MI-EXP-MIS-REB : mise au rebut. Lorsqu'une ressource informatique est amenée à quitter définitivement l'entité ou lorsqu'elle doit être réallouée, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, respecter des procédures établies en concertation avec l'ANSSI, ou selon des procédures dérogatoires autorisées et validées par le HFD.

⁵ <http://dnum.minint.fr/index.php/la-s-s-i/pes>

4.4. Lutte contre les codes malveillants

PSSIE-EXP-PROT-MALV : protection contre les codes malveillants. Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'entité. Ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux doit être corrélé.

PSSIE-EXP-GES-ANTIVIR : gestion des événements de sécurité de l'antivirus. Les événements de sécurité de l'antivirus doivent être remontés sur un serveur national pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

Les CSN doivent être destinataires de l'ensemble des alertes virales relevant de leur périmètre de compétences.

PSSIE-EXP-MAJ-ANTIVIR : mise à jour de la base de signatures. Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif prescrit par les services centraux.

PSSIE-EXP-NAVIG : configuration du navigateur Internet. Le navigateur déployé par l'équipe locale chargée des SI sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

MI-SAS-ANTIVIR : stations de décontamination antivirus. Afin d'assurer une meilleure dépollution des supports de stockage amovibles, des stations blanches de décontamination peuvent être mises en œuvre au profit des agents. Ces stations doivent être isolées du réseau bureautique ministériel, voire déployées sur un réseau ad hoc. Les bases antivirales des stations de décontamination doivent être mises à jour quotidiennement.

4.5. Mise à jour des systèmes et des logiciels

PSSIE-EXP-POL-COR : définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité. Le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini, et adapté suivant les contraintes et le niveau d'exposition du système.

PSSIE-EXP-COR-SEC : déploiement des correctifs de sécurité. Les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe locale chargée des SI en s'appuyant sur les préconisations et outils proposés par les services centraux.

MI-EXP-OBSOLET : assurer la migration des systèmes obsolètes. L'ensemble des logiciels utilisés sur le système d'information doit être dans une version pour laquelle l'éditeur assure le support, et tenu à jour des correctifs publiés, particulièrement ceux touchant au domaine de la sécurité. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

PSSIE-EXP-ISOL : isoler les systèmes obsolètes restants. Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et

pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation doit être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI).

MI-EXP-CODE-PROT : protection des codes sources et scripts. Il convient d'exercer un contrôle strict de l'accès au code source des programmes et tout autre script d'exécution afin d'empêcher l'introduction d'une fonctionnalité non autorisée et d'éviter toute modification involontaire. Dans la mesure du possible, des audits de code sont réalisés périodiquement.

4.6. Journalisation

MI-EXP-JOUR-SUR : journalisation des alertes. Chaque système doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre.

Les exigences légales et réglementaires en la matière doivent être prises en compte par les équipes projet et précisées dans les procédures d'exploitation.

PSSIE-EXP-POL-JOUR : définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces. Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le CSN, validée par l'autorité qualifiée, et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.

MI-EXP-CONS-JOUR : conservation des journaux. Les journaux des événements de sécurité doivent être conservés sur douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques. Celles-ci doivent systématiquement être précisées dans les procédures d'exploitation de sécurité.

MI-EXP-PROT-JOUR : Protection des journaux d'évènements. Les traces des journaux d'évènements doivent être centralisées et protégées en suppression ou modification. De telles actions ne doivent être possibles qu'aux seules personnes dûment habilitées et, dans la mesure du possible, différentes des personnes en charge des autres activités de production.

Le cas échéant, les opérations de chiffrement mis en place pour la protection des journaux doivent utiliser des mécanismes cryptographiques conformes aux annexes B du référentiel général de sécurité (RGS).

MI-EXP-JOURN-EVENT : journalisation systématique des évènements. Les événements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, aux actions d'administration sont systématiquement journalisés. Les chefs de projets, en collaboration avec les CSN, sont chargés de définir la granularité des journaux d'évènements utiles à la détection des incidents de sécurité. Le C2MI peut être sollicité pour assister les services dans cette tâche.

MI-EXP-DISPO-C2MI : mise à disposition des évènements. L'ensemble des journaux d'évènements utiles à la détection des incidents de sécurité et à l'analyse post-mortem d'un système doit être obligatoirement tenu à la disposition du C2MI.

5. Défense des systèmes d'information

Objectif A8-5 : défense des systèmes d'information. Défendre les SI nécessite une vigilance de tous, et des actions permanentes.

PSSIE-EXP-GES-DYN : gestion dynamique de la sécurité. L'équipe en charge de la SN doit procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information.

5.1. Gestion des matériels informatiques fournis à l'utilisateur

PSSIE-EXP-MAIT-MAT : maîtrise des matériels. Les postes de travail sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité de l'entité. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entité (qu'il s'agisse de mobiles, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels est interdite.

PSSIE-EXP-PROT-VOL : rappel des mesures de protection contre le vol. Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique du corpus de la PGSN-MI. Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr.

Il est recommandé de chiffrer les données contenues sur ces supports. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clé.

MI-EXP-DECLAR-VOL : déclarer les pertes et vols. Toute perte ou vol d'une ressource d'un système d'information ou d'un matériel professionnel doit être déclaré immédiatement au CSN et au C2MI.

MI-EXP-REAFFECT : réaffectation de matériels informatiques. Une procédure de gestion des équipements et supports de stockage dans le cadre de départs de personnel, de réaffectations à de nouveaux utilisateurs ou à d'autres systèmes, doit être mise en place et validée par le CSN.

Cette procédure doit définir les conditions de recours à un effacement des données, en utilisant une méthode préconisée ou un outil labélisé par l'ANSSI, ou de la mise en œuvre préalable et préventive de mécanismes de chiffrement des disques durs afin de simplifier les procédures. En aucun cas, un équipement ou un support du ministère doit être réaffecté à une personne externe au ministère de l'intérieur.

5.2. Nomadisme

MI-EXP-NOMAD-SENS : déclaration des équipements nomades aptes à traiter des informations sensibles. Seules les solutions de nomadismes dûment homologuées et validées par le HFD sont autorisées à traiter des informations sensibles.

Il appartient à l'autorité d'homologation de valider les usages possibles des équipements nomades vis-à-vis du système d'information dont il est responsable. Tout autre usage non explicitement autorisés est interdit.

Dans tous les cas, la doctrine d'emploi ministérielle relative au nomadisme doit être appliquée⁶.

⁶ Doctrine mobilité et nomadisme numérique, disponible sur le site <http://ssi.minint.fr/>

MI-EXP-ACC-DIST : accès à distance au système d'information de l'organisme. Sous réserve d'acceptabilité de l'autorité d'homologation, de respecter les exigences réglementaires en la matière⁷ et d'utiliser les solutions validées par le HFD, tout agent peut demander l'accès au télétravail pour accéder au système d'information du ministère.

5.3. Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

MI-EXP-IMP-SENS : impression des informations sensibles. Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur sur le déclenchement de l'impression jusqu'à la récupération du support imprimé. L'impression sécurisée peut se matérialiser par la saisie d'un code PIN personnel ou l'utilisation de la carte agent.

MI-EXP-IMP-2 : sécurité des imprimantes et copieurs multifonctions. Les imprimantes et copieurs multifonctions sont des ressources informatiques sensibles à part entière qui doivent être gérées en tant que telles. Elles ne doivent pas pouvoir communiquer avec l'extérieur, que ce soit pour des opérations de télémaintenance ou pour l'envoi de documents numérisés par courrier électronique.

6. Exploitation des centres informatiques

Objectif A8-6 : exploitation sécurisée des centres informatiques. Exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

6.1. Sécurité des ressources informatiques

Les règles suivantes sont présentées selon le modèle qui structure l'architecture des applications selon trois Tiers (Présentation – Application – Données).

Les socles techniques déployés dans chaque Tiers – en particulier les règles de sécurité à appliquer – sont précisés dans un cadre de cohérence technique (CCT) ministériel.

PSSIE-EXP-CI-OS: systèmes d'exploitation. Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque. Une attention particulière doit être apportée aux comptes administrateurs.

PSSIE-EXP-CI-LTP: logiciels en Tiers Présentation. La mise en œuvre d'une configuration renforcée est obligatoire sur les logiciels déployés pour le tiers présentation (ex: serveur Web, Reverse Proxy).

PSSIE-EXP-CI-LTA: logiciels en Tiers Application. Des règles de développement sécurisé, et les configurations des logiciels en Tiers Application doivent être fixées et appliquées. Elles sont détaillées dans le cadre de cohérence technique (CCT).

PSSIE-EXP-CI-LTD: logiciels en Tiers Données. Des règles très strictes (restrictions d'accès, interdictions de connexions, gestion des privilèges) s'appliquent aux logiciels en tiers données. Ces règles doivent être détaillées dans le cadre de cohérence technique (CCT).

⁷ Annexe B3 du RGS.

MI-EXP-LIV-LOG : protection de la livraison des logiciels et mises à jour. Des règles strictes doivent être mises en place (modalités de réception, vérification de l'intégrité, analyse antivirus, ...) concernant la procédure de livraison des logiciels et leurs mises à jour afin de prévenir les risques d'interception permettant à un attaquant d'introduire du code malveillant.

MI-EXP-CI-PROTFIC : passerelle d'échange de fichiers. Les échanges de fichiers entre applications doivent utiliser des protocoles sécurisés (TLS⁸, FTPS...) dans des versions à l'état de l'art. Les passerelles d'échanges ministérielles opérées par les DSI ministérielles doivent être utilisées.

PSSIE-EXP-CI-MESSTECH: messagerie technique. Pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite technique peut être déployée en zone de Back-office du centre informatique. Cette messagerie technique ne doit être en aucun cas utilisée directement par un utilisateur.

MI-EXP-CI-FILT: filtrage des flux applicatifs. De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre. Tout applicatif hébergé au sein des centres informatiques du ministère, doit passer par les chaînes de services des DSI ministérielles.

A défaut, il convient d'inclure dans les contrats d'hébergement tiers, les garanties suffisantes en termes de sécurité périmétrique (WAF, IPS, ...) permettant de protéger le patrimoine applicatif externalisé du ministère.

PSSIE-EXP-CI-ADMIN: flux d'administration. D'une manière générale, il convient de différencier deux types de flux d'administration: les flux d'administration de l'infrastructure (réservés aux agents du centre informatique) d'une part, les flux d'administration des applications métiers (réservés à la direction métier) d'autre part. L'attribution des droits d'administration doit respecter cette différenciation, et les 2 types de flux d'administration doivent être dans la mesure du possible cloisonnés.

PSSIE-EXP-CI-DNS: service de noms de domaine – DNS technique. Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes au centre informatique, on utilisera les extensions sécurisées DNSSEC.

PSSIE-EXP-CI-EFFAC: effacement de support. Le reconditionnement et la réutilisation des disques durs pour un autre usage (ex: réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.

PSSIE-EXP-CI-DESTR: destruction de support. La fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur...) doit s'accompagner d'une opération de destruction avant remise au constructeur.

PSSIE-EXP-CI-TRAC: traçabilité / imputabilité. Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation emploient une référence de temps commune (service NTP, Network Time Protocol).

MI-EXP-CI-SUPERVIS : supervision. Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place. Les DSI ministérielles doivent mettre en œuvre des infrastructures centralisées pour la supervision de leurs centres informatiques et des applications hébergées, conformément aux recommandations de l'ANSSI.

⁸ Recommandations de l'ANSSI pour un déploiement et une utilisation sécurisés de TLS : https://www.ssi.gouv.fr/uploads/2017/07/anSSI-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf

PSSIE-EXP-CI-AMOV: accès aux périphériques amovibles. Il convient de stocker tous les supports dans un environnement sûr et sécurisé afin d'éviter tout accès malveillant à son contenu, plus particulièrement si la confidentialité des données constitue un facteur important ou s'ils sont utilisés pour des opérations d'exploitation. Le chiffrement de son contenu peut aussi nécessaire notamment lorsqu'il a besoin d'être transporté.

PSSIE-EXP-CI-ACCRES: accès aux réseaux. Dans un centre informatique, le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, etc.) font l'objet de procédures sécurisées.

MI-EXP-CI-AUDIT: audit/contrôle. Le CSN pilote des audits réguliers des systèmes d'information relevant de sa responsabilité, en conformité avec la méthode retenue par la démarche d'intégration de la sécurité dans les projets (DISSIP). Des scans de vulnérabilités automatiques peuvent être réalisés périodiquement, sous réserve que les solutions utilisées soient validées par l'ANSSI, par le cadre de cohérence technique (CCT) ministériel ou à défaut, par le SHFD.